First Security Islami Bank Limited
ICT Division
Head Office
Plot#12, 2ⁿᵈ & 3ʳᵈ Floor, Main Road.
Block # A, P.S- Badda,
Bashundhara R/A, Dhaka-1229.
Web: www.fsiblbd.com; email: ictp@fsiblbd.com

Ref: FSIBL/HO/ICT/199/2022

Date: 06.04.2022

REQUEST FOR PROPOSAL (RFP)

Purchasing of Network Management System (NMS) at DC & Disaster Recovery (DR) Site for 03 (Three) years

Bidder Reg. No.

Section A: General Information

SN	Item	Description				
1	Name of the Bank	First Security Islami Bank Limited				
2	Procuring Entity Name	Information & Communication Technology Division				
3	Invitation of tender for	Supply & implementation of **Network Management System (NMS) at DC & Disaster Recovery (DR) Site** as per technical specifications detailed in "Section C".				
4	Invitation for Quotation Ref. & Date	FSIBL/HO/ICT/199/2022 Date: 06.04.2022				
5	Procurement Method	Open Tendering Method				
6	Source of Fund	First Security Islami Bank Limited				
7	Registration of bidders & price of Tender Document:	The interested eligible bidders have to enroll their name by submitting a prayer along with a non-refundable registration/enrollment fee **Tk.2,500.00 (Taka Two Thousand Five Hundred only)** in the form of "Payment Order" in favor of "First Security Islami Bank Limited" during submission of tender. No Tender documents will be sold physically. The bidder have to copy or download this tender documents from the website: www.fsiblbd.com and place them on their own letterhead to submit their bid.				
8	Tender Process Dates & Times		Registration		Submission		Opening Time
		Tender Process	Start	End	Start	End	
		Date	06.04.2022	27.04.2022	27.04.2022	27.04.2022	27.04.2022
		Time	10.30 AM	02:00 PM	10:30 AM	03:00 PM	03:30 PM
	Pre-bid Schedule	Date	17.04.2022				
		Time	11.00 AM				
9	Place of Pre-bid meeting, tender submission & opening	First Security Islami Bank Limited, Plot#12, 3ʳᵈ Floor, Main Road. Block # A, P.S- Badda, Bashundhara R/A, Dhaka-1229.				
10	Composition of bid Price shall be inclusive of	The costs of complete integration of Network Management System (NMS) as instructed by the bank, testing, commissioning, delivering to directed site and admissible VAT, excise duty, subsidiary duty, import duty, VAT, AIT etc. all types of taxes and revenues of the government and other regulatory authorities along with time value of money up to settlement of bills taking clearances from the end user of the bank.				
11	Awarding the successful bidder	The bank may negotiate with the successful bidder or all bidders regarding price reduction modification if necessary before issuing the acceptance letter. A notification of award (NOA) will be provided by Bank to the successful bidder. Within 07 days of receipt of the Letter of Acceptance, the successful bidder shall sign a copy of it and return to the bank. Work must be completed within the time specified in the Work Order/Contract.				
12	Payment & Security	The bidder shall furnish as bid security of 2.50% of the total financial offer in the form				

Signature & Seal of the bidder

		of bank draft or bank guarantee in the form of pay order or bank guarantee from any scheduled bank in favor of First Security Islami Bank Limited. The bid security shall be submitted along with the tender inside the envelop marked as "Financial Offer- for Purchasing of Network Management System (NMS) The bid security should be valid for 60 days from the date of bid opening. Any bid not accompanied by an acceptable bid security shall be rejected as non-responsive. The bid security of unsuccessful bidders will be returned within 7 days from the date awarding the successful bidder. The bid security of the successful bidder will be returned when the bidder has signed the NOA and furnished the required performance security. The bid security may be forfeited if (a) the bidder withdraws its bid during the period of bid validity specified in the bid form; (b) if a successful bidder fails to sign the contract and (c) if a successful bidder fails to furnish the performance security.
		Within 07 days of receipt of the notification of award from the Bank, the successful bidder shall furnish as performance security of 10% of total amount in the form of pay order or bank guarantee from any scheduled bank in favor of First Security Islami Bank Limited. The performance security should be valid till the successful competition of the project including products delivery & service integration to its full extent.
		Bid shall remain valid for a period of 3 (Three) months after the date of opening of the proposals. In exceptional circumstances, prior to expiry of the original bid validity period, the Bank may request the bidder to extend the period of validity for a specified additional period. The request and the responses shall be made in writing. A bidder agreeing to the request will not be permitted to modify its bid.
		50% payment of total price may be provided as an advance payment upon request of the successful bidder. 50% payment may made after implementation of Network Management System (NMS) in its environment for DC & Disaster Recovery (DR) Site upon getting satisfactory certificate from ICT Division, FSIBL, Head Office expressing clearly that the end user has no objection.
		In case of a failure of the successful Bidder to implement of N Network Management System (NMS) in the prescribed time, the bidder will be liable to pay 0.5% of the Contract price as liquidated damages for every week after the deadline and will be deducted from the bill amount. The maximum penalty will be 10% of total contact price.
13	**Submission of bidders Qualifications/Eligibility and curse of bidder**	The interested registered bidder shall copy the "bidders' qualification" form from the webpage and place them on their own letterhead write their qualifications and individual information in a separate sealed envelope with proper labeling mentioning- "Bidder's Qualifications /Eligibility for supplying & implementation of Network Management System (NMS), Name of the bidder & Registration No.
14	**Submission of Technical & Financial Offer**	The interested registered bidder shall copy the asked Technical Specifications and Financial Offer form from the webpage and place them on their own letterhead and write their price offer for Section "C" in the designated field(s) and submit the document in a separate sealed envelope with proper labeling mentioning- "Financial Offer- for Purchasing of Network Management System (NMS), Name of the bidder & Registration No.
15	**Name and address of the Office for receiving tender(s)**	Vice President & Head of ICT Division (C.C.). First Security Islami Bank Limited, Plot#12, 3rd Floor, Main Road. Block # A, P.S- Badda, Bashundhara R/A, Dhaka-1229.
16	**Address of Official Inviting Tender**	Do.
17	**Contact Details**	Telephone No. 02-8432613-22 Ext: 301, 304 email: ictp@fsiblbd.com

18	**Special Instruction**	The Bank Authority reserves the right to -
		  1. Explain or clarify the terms of this tender notice in its own way,
		  2. Bring necessary changes in the notice
		  3. Increase or decrease the tender quantity
		  4. Reject the lowest
		  5. Reject any or all bids
		  6. Select any bidder deems fit and proper by them
		  7. Bidder have to bid full of the Section "C"
		The bank authority can perform all the above things without assigning any reason. The bidder/supplier shall have no right to challenge the decision of the Bank Authority in

Signature & Seal of the bidder

		any court of law or to any arbitrator.

REQUEST FOR PROPOSAL (RFP)

Purchasing of Network Management System (NMS) at DC & Disaster Recovery (DR) Site for 03 (Three) years

Tender Ref: FSIBL/HO/ICT/199/2022
Date: 06.04.2022
Bidder Reg. No.

Section B: Bidder's Information and Qualifications/Eligibility

SN	Description	Qualification	Response	Remarks
01	Name of the Bidder	Required		Attach NID copy
02	Designation of the Bidder	Required		
03	Company Name	Required		
04	Company Type [Proprietorship, Partnership, Private Limited, Public Limited etc.]	Required		
05	Website address of the company	Required		
06	Bidder's Office Phone No.	Required		Attach bill copy
07	Bidder's email address	Required		Send "Test" mail to ictp@fsiblbd.com
08	Bidder's Mobile No.	Required		
09	Verified Business Address	Required		Attach proof
10	Name of Contact Person	Required		Attach NID copy
11	Designation of the contact Person	Required		
12	Official email address	Required		Send "Test" mail to ictp@fsiblbd.com
13	Valid Trade License No.	Required		Attach proof
14	Valid VAT Registration No.	Required		Attach proof
15	Valid ETIN	Required		Attach proof
16	Valid IRC No.	Required		Attach proof
17	Authorization of the Principal	Required		Attach proof
18	Bank solvency certificate	Required		Attach proof
19	Are you adequately solvent to sale on? Credit for a period of 6 months or more?	Yes/No.		
20	Experience: The bidder must have 5 years of experience for supplying similar hardware & license in at least 3 different commercial Banks of Bangladesh.	Required Bank- WO- Date- Quantity-		Attach proof
21	Are you Banned by any bank authority or? Government agency?	Yes/No		

Statement of the bidder: All the above information provided hereinabove are true. We will supply the order from genuine, valid and lawful sources and will pay all admissible VAT, Tax & other duties as per rule of the Government of Bangladesh.

Signature & Seal of the bidder

REQUEST FOR PROPOSAL (RFP)

Purchasing of Network Management System (NMS) at DC & Disaster Recovery (DR) Site for 03 (Three) years

Tender Ref: FSIBL/HO/ICT/199/2022
Date: 06.04.2022
Bidder Reg. No

Section C: Technical/Financial Specifications of Network Management System (NMS)

S.No	Network Management System-(Performance Monitoring)		
	Description	Compliant/ Non-compliant	Remarks
1	**Core Monitoring Capabilities**		
1.1	The proposed monitoring solution should be able to monitor: (a) Routers (b) Switches (c) Firewalls (d) Wireless devices (e) Servers (e) Other SNMP-enabled devices		
1.2	Should automatically provide real-time, in-depth network performance statistics after discovery/configuration of devices, including but not limited to, (a) CPU load (b) Memory utilization (c) Interface utilization (d) packet loss		
1.3	Should show statistics like interface bandwidth, current traffic in bps, total bytes received/transmitted etc.		
1.4	Should be able to discover and troubleshoot network paths hop-by-hop for both on premises and cloud environment for specific TCP connections		
1.5	Should display information including alerting for major routing protocols (BGP, OSPF , RIP, EIGRP) with options to view and search routing tables including VRFs, changes in default routes and flapping routes, router topology and neighbor statuses		
1.6	Should help with multicast traffic information monitoring, alerting including topology information, multicast information, route information, multicast errors etc.		
1.7	Should display device status and interface status by different colors to represent warning and critical status		
1.8	Should monitor hardware health for popular vendors like Cisco, DELL, F5, Juniper, HP etc. and should allow alerting and reporting on hardware health monitoring		
1.9	Should show both real time details and historical details in form of charts with option to choose the time periods		
1.10	Should be able to discover and monitor both IPv4 and IPv6 devices		
1.11	Should have options to poll using SNMP v1, v2c and v3 and WMI		
1.12	Should have options to configure polling intervals as needed		
1.13	Should have options to specify data retention periods		
1.14	Should have the option to determine device availability using SNMP only		
2	**Network Discovery**		
2.1	The proposed monitoring solution should be able to discover devices in the network with SNMP and ICMP capabilities automatically, on input of, (a) IP address ranges (b) subnets (c) individual IP addresses (d) Active Directory		
2.2	Should not add devices with multiple IP addresses as duplicate nodes but should list all known IP addresses for the node		
2.3	Should allow interface filtering on discovery results to exclude virtual interfaces and access ports and select interfaces based on pattern matching		
2.4	Should have option to automate and schedule discovery process		
2.5	Should be able to automatically imports discovered devices		
2.6	Should prompt in web console on discovery of new devices in network		
2.7	Should use discovered information for creating topology maps		
3	**Graphical User Interface and Customization**		

Signature & Seal of the bidder

3.1	The proposed management solution Should provide a high-quality graphical user interface with asynchronous view refreshing		
3.2	This web console should be accessible centrally or remotely		
3.3	The web console should allow multiple users to log in at the same time		
3.4	It should have horizontal scaling options available if too many users login at same time		
3.5	It should allow customization by having options to add/remove sections in web pages as necessary		
3.6	It Should provide a unified view of alerts, traps, events, syslog messages in a single page		
3.7	It should give a single unified view of multicast information, route information and device information for a device.		
3.8	It should quickly highlight devices with issues, based on different properties like response time, cpu load, memory usage, high interface usage etc.		
3.9	It should allow creation of custom dashboards and restrict views for users based on devices or interfaces, i.e. it should have role-based access		
3.10	It should log user actions and events in the web console for audit purposes and they should be available for alerting and reporting		
3.11	It should allow interactive charting for node, interface, volume charts etc.		
3.12	It Should provide a dynamic dashboard that allows in-depth visibility and correlates disparate historical data points across different part of the infrastructure. The result should be exportable in tabular format		
3.13	It should allow export of any web page in console to PDF format		
3.14	It should integrate with Active Directory for user login purposes		
3.15	It should be easy to use and intuitive with drill-down features		
4	**Advanced Reporting**		
4.1	The proposed monitoring solution Should provide current and historical out-of-the-box reports for various statistics monitored		
4.2	Should be able to generate / create the report via the web console		
4.3	Should be able to generate statistical reports that can be used as reference for future planning or troubleshooting		
4.4	Should allow customization of reports by adding/removing columns, setting filters, specifying timeframes, grouping columns etc.		
4.5	Should allow advanced customization by providing options to enter custom queries to query the database directly		
4.6	Should have options to save the customized reports permanently and have them accessible in web console		
4.7	Should allow reports to be sent out on schedule as daily, weekly, monthly reports		
4.8	Should allow emailing of dashboards created in web console		
4.9	Should be able to configure both charts and tables into a single report.		
4.10	Should have options to import/exports reported created by other users		
4.11	Should support multiple formats such as pdf, HTML and CSV		
5	**Advanced Alerting**		
5.1	The proposed monitoring solution should be able to manage and display events/alerts in the web console		
5.2	The alerts and events information should be logged into the database for future reference		
5.3	The alerting mechanism should allow complex conditions and condition groups to be specified for narrowing down the alert condition		
5.4	It should allow custom queries to be entered to create rules against the database		
5.5	It should allow creation of new alerts from scratch and also customizable threshold limits		
5.6	It should allow creation of alerts based on sustained states		
5.7	Should have various actions that can be taken, including but not limited to, sending out emails, forwarding SNMP traps, running executable, sending SMS text alerts, playing sound, emailing a web page etc.		

Signature & Seal of the bidder

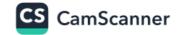|			
5.8	Should have support for variables in alert email message to make the content more self-explanatory		
5.9	Should have the ability to dynamically baseline statistics and automatically set Warning and Critical threshold		
5.10	Should allow alerts suppression during scheduled maintenance		
6	**Grouping**		
6.1	The proposed monitoring solution should allow grouping of devices by various properties -- by department, by location, by name and by other properties gathered		
6.2	Should also allow adding members to groups on-the-fly by specifying a property which can dynamically change values, like volumes reaching low free space		
6.3	Should be able to define dependencies and relationships between connected devices and interfaces to avoid false-positive email alerts in case of outage.		
6.4	Should be able to calculate group availability by averaging the availability of the group members.		
7	**Network Maps**		
7.1	The proposed monitoring solution should be able to represent the network pictorially and display performance details of devices in real time		
7.2	Should allow customization of background, icons etc. and should allow multiple network maps to be nested with drill-down capabilities		
7.3	Should be able to display not just the device status on the map but also status of any other detail obtained through custom MIB polling		
7.4	Should have the capability to display the status of nodes or an aggregated group of nodes over dynamically updated street data.		
7.5	Should be able to automatically connect devices by means of topology information gathered during discovery, like Cisco Discovery Protocol or Link Layer Discovery Protocol		
7.6	Should be able to view multicast topology using upstream and downstream device list information		
7.7	Should be able to display devices location on the geographical level and down to street level		
7.8	Should have the ability to show the link utilization as a 'weather map'		
8	**Multi-vendor Support**		
8.1	The proposed monitoring solution should not be vendor-specific		
8.2	The discovered devices should be detected as that of a specific vendor and categorized automatically		
9	**Extensibility**		
9.1	The proposed monitoring solution should allow gathering of custom properties from SNMP-enabled devices by specifying the OID of the properties		
9.2	Should be able to fetch properties from devices without need to import device MIBs into MIB database		
9.3	Should be able to get real time values, charts and also alerts on these custom properties		
9.4	Should have APIs available to programmatically import/export nodes and do similar functionality		
10	**Application Aware Network Performance Monitoring**		
10.1	Should be able to provide Network Response Time (NRT) and Application Response time (ART) for critical applications		
10.2	Should be able to identify and classify ~1200 applications out of the box		
10.3	Should have the ability to display aggregate volume metrics per application / node		
10.4	Should have the ability to create custom HTTP applications		
10.5	Should be able to contextually provide QoE data for nodes in Node Details sub view		
11	**Additional Components**		
11.1	Should have utilities to view the database, to stop and start application services		
11.2	Should have options to receive, display and alert on syslog messages and traps from devices		

Signature & Seal of the bidder

11.3	Should have wireless reporting option to display wireless thin and autonomous access points and their associated clients		
11.4	Should have customized mobile views of console for administrators' immediate viewing		
11.5	Should be able to monitor Cisco switch stack, with the ability to display individual member switches, power stack and data stack rings		
11.6	Should be able to report on technologies like Cisco UCS, Energy wise feature		
11.7	Should be able to report on virtualized Cisco Nexus 1000V switches, VSAN, Fibre Channel switches like Cisco MDS, Brocade, McData devices		
11.8	Should be able to monitor cloud-based Meraki wireless infrastructure		
11.9	Should be able to monitor entire VMware and Hyper-V virtual infrastructure, including Virtual Centers, Datacenters and ESX clusters, and automatically track VM performance		
11.10	Should be able to monitor individual components in F5 BIG-IP load balancing environment		
11.11	Should be able to monitor individual components in Cisco ASA firewall, including but not limited to: connection count, site to site and remote access VPN tunnels, interface identity and utilization, high availability status and configuration synchronization status.		
11.12	Should be able to monitor Cisco Nexus with VDC awareness, including vPC specific view for configured vPC and peer vPC.		
11.13	Should be able to monitor SDN environment (e.g. Cisco ACI), including but not limited to: APICs, tenants, application profiles, endpoint group and physical entities.		
12	**Integration**		
12.1	Should be able to integrate with modules serving other monitoring purposes and provide a single-pane-of-glass view		
12.2	Should allow integration with third-party applications at user-interface layer, through message exchanges and also through APIs		
12.3	Should be able to integrate with Service Now, with the ability to automatically create incidents and synchronize the acknowledgement of incidents bidirectional		
12.4	It should support SAML 2.0 for integration with Active Directory Federation Services (AD FS) or Okta for Single Sign-On (SSO)		
13	**Enterprise Scalability**		
13.1	The proposed monitoring solution should be able to accommodate growth through addition of load-balancing applications		
13.2	Load-balancing engines should handle interruptions in the connection between the engines and the main application		
13.3	Should allow information from multiple instances of application to be consolidated into a single view		
13.4	Should support multiple deployment options: (a) Centralized deployment (b) Distributed deployment (c) Hybrid deployment With a centralized operations console view, alert acknowledgement and reporting interface		
14	**High Availability**		
14.1	Should have options for ensuring high-availability of application, with/without use of failover products		
15	**Platform Security**		
15.1	Should be fully compatible with TLS 1.2, without any dependency on TLS 1.1 or 1.0		
15.2	Should support Microsoft Device Guard with all binary signed to ensure code integrity		
16	**Deployment**		
16.1	Should be deployable within one hour and should not require consultants for deployment, implementation, configuration or customization		
16.2	Should support agentless deployment		
16.3	Should support deployment on Amazon EC2 and Microsoft Azure (optional)		

Signature & Seal of the bidder

		Compliant/Non-compliant	Remarks
16.4	Should support centralized upgrade for all remote components (e.g. remote data collectors, web consoles) without additional management operation on the remote servers		
16.5	Should include actionable dashboard that provide self check functionality for the monitoring platform and display remediation advice for non-compliant item		
17	**Frequency of Updates**		
17.1	New features to be added to product versions frequently, preferably twice every year or more		
17.2	Should notify availability of new versions in the web console		
18	**Product Support**		
18.1	Should provide 24x7 support		
18.2	Active support through forums and community would be a welcome feature		

Network Management System-(Application Monitoring)

S.No	Description	Compliant/Non-compliant	Remarks
1	**Core Monitoring Capabilities**		
1.1	The proposed monitoring solution should be able to monitor: (a) Application status (b) Application performance statistics (c) Services and processes (d) OS performance (e) Hardware		
1.2	Should automatically provide real-time view of processes running in systems and in-depth application performance statistics after discovery/configuration of applications		
1.3	Should be able to manage the processes, services running in systems and in-depth application performance statistics after discovery/configuration of applications		
1.4	Should automatically provide real-time view of windows event logs including the level of the event logs, Event ID, and source.		
1.5	Should have expert monitoring methods that point out the status and performance of key parameters (like services, queue length in case of Exchange, sql queries in case of databases etc.) of applications based on best practices		
1.6	Should be able to put together important parameters of an application, into one single monitoring template that can be uniformly applied to applications on different servers		
1.7	A customization made in one application's monitoring template should be propagated immediately to all other servers having that application		
1.8	Should allow use of custom scripts with various scripting engine options like VBscript, Perl, Powershell etc.		
1.9	Should have options for user experience monitoring for various applications and services like HTTP, FTP, DHCP, DNS, SQL Server, Oracle, JSON, etc. to find out issues even before users notice them		
1.10	Should be able to report on hardware details (like CPU, memory, fan state, power etc.) of servers from popular vendors like IBM, HP, DELL and also VMware Hosts		
1.11	Should have options to poll using SNMP, WMI and other methods		
1.12	Should display application status and status of important services by different colors to represent warning and critical status		
1.13	Should show both real time details and historical details in form of charts with option to choose the time periods		
1.14	Should have options to configure polling intervals as needed		
1.15	Should be able to get Disk I/O Performance Metrics for Processes & Services Monitored via WMI		
1.16	Should have options to specify data retention periods		

Signature & Seal of the bidder

1.17	Should be able to provide User Audit Event Logging including Terminated Processes, Stopped/Started/Restarted Services, Nodes Rebooted Newly Created/Edited/Deleted Credentials & Application Templates Assigned, Removed, Managed, and Unmanaged Applications			
2	**Cloud Monitoring Capability**			
2.1	Discover and monitor EC2 cloud instances and EBS volumes in AWS via API			
2.2	Discover and monitor Azure cloud service via API			
2.3	Automatically discover and monitor new instances			
2.4	Consolidate view for cloud, hybrid, and on-premises systems			
2.5	Monitor application performance and OS metrics on cloud instances			
2.6	Should be able to monitor Docker, Docker Swarm, Kubernetes, and Apache Mesos container deployments, with the ability to automatically discover containers running on the orchestrator.			
3	**Application Discovery / Monitoring**			
3.1	The proposed monitoring solution should be able to discover applications in the chosen servers, apply monitoring for them and start report statistics in few minutes			
3.2	Should have option to find processes either through WMI or SNMP, Performance Counter Monitors, WMI Monitors, VMware Performance Counter Monitors etc.			
3.3	Should be able to discover application dependencies and connections between application servers, with the ability to monitor both incoming and outgoing connection information on a per process level.			
3.4	Should have option to discover JMX monitors for monitoring Java-based applications like JBoss, Tomcat, WebLogic etc.			
3.5	Should be able to discover email and directory servers, databases, network services, operating systems, VMware ESX servers etc. automatically by means of inbuilt monitoring templates			
3.6	Should be able to create and set automatic Calculation of Warning & Critical Thresholds From Baseline Data			
3.7	Should provide in depth monitoring of Microsoft SQL out of the box with the following SQL Error Logs, Individual Database Details Views, Status of SQL Agent, Job Results, Index Fragmentation, SQL Server Connections			
3.8	Should provide in depth monitoring of Microsoft Exchange mailbox role servers including performance of Information store, database, storage, replication, etc. It should also trend the sent and received emails and attachments for every mailbox user.			
3.9	Should provide in depth monitoring of Microsoft Internet Information Service (IIS) including services, processes, individual website connections and response time, individual application pool, other statistic like cache and connection.			
3.10	Should provide in depth monitoring of Microsoft Office 365 products including Exchange Mailboxes, mail Traffic, security, subscription status and mobile device statistics.			
4	**Graphical User Interface and Customization**			
4.1	The proposed management solution Should provide a high-quality graphical user interface			
4.2	This web console should be accessible centrally or remotely			
4.3	The web console should allow multiple users to log in at the same time			
4.4	It should have horizontal scaling options available if too many users login at same time			
4.5	It should allow customization by having options to add/remove sections in web pages as necessary			
4.6	It Should provide a unified view of alerts, traps, events etc. in a single page			
4.7	It should quickly highlight applications with issues, based on different properties like down applications, applications with problems, parameters with high CPU, memory usage etc.			
4.8	It should allow creation of custom dashboards and restrict views for users based on applications, i.e. it should have role-based access			
4.9	It should allow interactive charting			
4.10	It should allow export of any web page in console to PDF format			

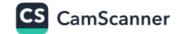|				
4.11	It should integrate with Active Directory for user login purposes			
4.12	It should be easy to use and intuitive with drill-down features			
4.13	It should have integration options to automatically visualize relevant virtual infrastructure objects such as data stores and storage objects such as LUNs			
4.14	Should provide a dynamic dashboard that allows in-depth visibility and correlates disparate historical data points across different part of the infrastructure. The result should be exportable with a tabular format.			
5	**Advanced Reporting**			
5.1	The proposed monitoring solution Should provide current and historical out-of-the-box reports for various statistics monitored			
5.2	Should be able to generate / create the report via the web console			
5.3	Should be able to generate statistical reports that can be used as reference for future planning or troubleshooting			
5.4	Should allow customization of reports by adding/removing columns, setting filters, specifying timeframes, grouping columns etc.			
5.5	Should allow advanced customization by providing options to enter custom queries to query the database directly			
5.6	Should have options to save the customized reports permanently and have them accessible in web console			
5.7	Should allow reports to be sent out on schedule as daily, weekly, monthly reports			
5.8	Should allow emailing of dashboards created in web console			
5.9	should be able to configure both charts and tables into a single report.			
5.10	Should have options to import/exports reported created by other users			
5.11	Should support multiple formats such as pdf, HTML and CSV			
6	**Advanced Alerting**			
6.1	The proposed monitoring solution should be able to manage and display events/alerts in the web console			
6.2	The alerts and events information should be logged into the database for future reference			
6.3	The alerting mechanism should allow complex conditions and condition groups to be specified for narrowing down the alert condition			
6.4	It should allow custom queries to be entered to create rules against the database			
6.5	It should allow creation of new alerts from scratch and also customizable threshold limits			
6.6	It should allow creation of alerts based on sustained states			
6.7	Should have various actions that can be taken, including but not limited to, sending out emails, forwarding SNMP traps, running executable, sending SMS text alerts, playing sound, emailing a web page etc.			
6.8	Should have support for variables in alert email message to make the content more self-explanatory			
7	**Grouping**			
7.1	The proposed monitoring solution should allow grouping of applications by various properties -- by department, by location, by name and by other properties gathered			
7.2	Should also allow adding members to groups on-the-fly by specifying a property which can dynamically change values, like volumes reaching low free space			
7.3	Should be able to define relationships between servers and applications to avoid false-positive email alerts in case of outage.			
8	**Topology Maps**			
8.1	The proposed monitoring solution should be able to represent the applications pictorially and display performance details of applications in real time			
8.2	Should allow customization of background, icons etc. and should allow multiple maps to be nested with drill-down capabilities			
9	**Multi-vendor Support**			
9.1	The proposed monitoring solution should not be application-specific			
9.2	The discovered applications should be monitored with inbuilt monitoring templates created based on best practices			

Signature & Seal of the bidder

10	Extensibility		
10.1	The proposed monitoring solution should allow custom scripts to be included to extend application monitoring capabilities		
10.2	Should be able to get real time values, charts and also alerts on these custom properties		
10.3	Should have APIs available to programmatically import/export nodes and do similar functionality		
11	Additional Components		
11.1	Should have utilities to view the database, to stop and start application services		
11.2	Should have customized mobile views of console for administrators' immediate viewing		
12	Integration		
12.1	Should be able to integrate with modules serving other monitoring purposes and provide a single-pane-of-glass view		
12.2	Should integrate with virtualization monitoring software to provide end-to-end application performance view from the application to the VM to the host.		
12.3	Should allow integration with third-party applications at user-interface layer, through message exchanges and also through APIs		
12.4	Should be able to integrate with Service Now, with the ability to automatically create incidents and synchronize the acknowledgement of incidents bidirectional		
12.5	It should support SAML 2.0 for integration with Active Directory Federation Services (AD FS) or Okta for Single Sign-On (SSO)		
13	Enterprise Scalability		
13.1	The proposed monitoring solution should be able to accommodate growth through addition of load-balancing applications		
13.2	Load-balancing engines should handle interruptions in the connection between the engines and the main application		
13.3	Should allow information from multiple instances of application to be consolidated into a single view		
13.4	Should support multiple deployment options: (a) Centralized deployment (b) Distributed deployment (c) Hybrid deployment With a centralized operations console view, alert acknowledgement and reporting interface		
14	High Availability		
14.1	Should have options for ensuring high-availability of application, with/without use of failover products		
15	Platform Security		
15.1	Should be fully compatible with TLS 1.2, without any dependency on TLS 1.1 or 1.0		
15.2	Should support Microsoft Device Guard with all binary signed to ensure code integrity		
16	Deployment		
16.1	Should be deployable within one hour and should not require consultants for deployment, implementation, configuration or customization		
16.2	Should support agentless deployment		
16.3	Should include optional agent for Windows, Linux (x86), Linux (ARM) and AIX		
17	Frequency of Updates		
17.1	New features to be added to product versions frequently, preferably twice every year or more		
17.2	Should notify availability of new versions in the web console		
18	Product Support		
18.1	Should provide 24x7 support		
	Bidder should offer min 300 Node license from Day 1.		
18.2	Active support through forums and community would be a welcome feature		

Signature & Seal of the bidder

Section D: Training on Network Management System (NMS)

Training Name	Persons
In depth Training on Network Management System (NMS)	06 (Six)

** The above mentioned price is inclusive of all costs, taxes & VATs as per rule of the government of Bangladesh.

Name of the Bidder   :
Designation of the Bidder :
Company Name   :
Business Address   :
Mobile No.   :

Signature & Seal of the bidder